



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/704,418	11/01/2000	Vincent J. McCullough	15-0230	4634
20457	7590	01/06/2005	EXAMINER	
ANTONELLI, TERRY, STOUT & KRAUS, LLP			ARANI, TAGHI T	
1300 NORTH SEVENTEENTH STREET			ART UNIT	
SUITE 1800			PAPER NUMBER	
ARLINGTON, VA 22209-9889			2131	

DATE MAILED: 01/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

**Application No.**

09/704,418

**Applicant(s)**

MCCULLOUGH ET AL.

**Examiner**

Taghi T. Arani, Ph.D.

**Art Unit**

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 27 July 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-28 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- ☐ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date August 26 2004.
- ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- ☐ Notice of Informal Patent Application (PTO-152)
- ☐ Other: \_\_\_\_\_.

### **Detailed Action**

Claims 1-28 are pending in the application.

### **Response to Arguments**

Applicant's arguments filed on 7/27/2004 regarding the rejection of the have been fully considered but they are not persuasive.

Applicant's attempt to distinguish the claims from prior art is based on noting the lack of a teaching of a "registration web server" and Cordery's failure to teach any requesting of the registration web server to revoke a user signature certificate, as recited in claim 1.

Applicant further argues "the Office Action also relies on 608 of FIG. 6 for issuing a signed message to postage and certificate meter to revoke the certificate. However, the signed message being issued in connection with step 608 of Cordery does not disclose that the signed message be sent to a registration web server, but instead Cordery teaches that the signed message is sent to a postage meter subsystem 218 (Col. 8, lines 16-19). Nothing in Cordery teaches or even suggests that the postage meter is a web server.", REMARKS, page 10, 2<sup>nd</sup> paragraph

The Examiner responds that Cordery discloses that "a postage and certificate meter combines the functionality of a postage meter and a certificate management device, providing significant advantage to the postal service (and other certification authorities) and to the user. The postage and certificate meter is a secure cryptographic device with secret information that allows secure communication with the certificate authority such as a post office or other trusted third party and capability to use, manage and execute various security services, col. 3, lines 44-47.

According to the MPEP 904.01, the Examiner is obligated to give each term in the claims its broadest reasonable interpretation. See also *In re Morris*, 127 F.3d 1048, 44 USPQ2nd 1023 (Fed. Cir. 1997) . That is, Cordery's certificate management device inherently carries out the recited steps and functionality of a' registration web server" .

Applicant argues that Cordery "provides no teaching (or even a suggestion) that any communication, including a request to a certificate authority is provided as a request to a registration web server over the authenticated secure channel, as recited in claim 1.", page 10, 1st paragraph.

The Examiner responds that Cordery's postage and certificate meter is a secure cryptographic device with secret information that allows secure communication with the certificate authority such as a post office or other trusted third party and capability to use, manage and execute various security services, col. 4, lines 1-8. That is, Cordery's disclosed secure communication constitutes (reads on) the recited "authenticated secure channel".

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1,18 and 23-25 are rejected under 35 U.S.C. 102(e) as being anticipated by Cordery et al. (U.S. Patent 6,134,328 and Cordery hereinafter).

**In regards to claim 1**, Cordery teaches a method for revocation of a signature certificate in a Public Key Infrastructure (PKI) (figure 6) comprising:

creating an authenticated secure channel with a registration web server (figure 6, step 604);

requesting the registration web server revoke a user signature certificate, the requesting occurring over the authenticated secure channel (figure 6, step 608);

revoking the user signature certificate (figure 6, step 616); notifying a directory by the registration web server of revocation of the user signature certificate (figure 6, steps 620 and 624); and

setting a user entry in the directory to a state without a signature certificate (figure 6, step 622).

**In regards to claim 18**, the claim limitations recite an apparatus ( A server comprising a storage medium) having instructions to substantially execute the method of claim 1, therefore the same rejection applies.

In regards to claims 23-25, the claim limitations recite a system to substantially execute the method of claim 1, therefore the same rejection applies.

#### Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill

Art Unit: 2131

in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 2-4, 7, 21 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cordery in view of Grimmer (U.S. Patent 5,774,552).

**In regards to claim 2**, Cordery teaches the system of claim 1 as discussed above.

Cordery does not teach generating a directory password for the user during creation of the user signature certificate.

Grimmer discloses a system for retrieving X.509 certificates from an X.509 directory service agent (col. 1, lines 9-10).

Grimmer teaches generating a directory password for the user during creation of the user signature certificate (i.e. if a UserPassword attribute type was defined to hold user password information in the X.500 directory, user2 can query the directory to verify that the password it received from user1 matched the one held in the X.500 directory) (col. 4, lines 48-52).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the teaching of Cordery with the teachings of Grimmer to include generating a directory password for the user during creation of the user signature certificate with the motivation to provide a basis for authentication and security services (Grimmer, col. 4, lines 32-34).

**In regards to claims 3, 21 and 26**, Cordery teaches that the creating and requesting are initiated by the user (i.e. [the revocation] may occur, for example, where an individual believes that his or her private key has been compromised) (col. 8, lines 7-9).

**In regards to claim 4**, Cordery teaches that the creating and requesting are initiated by the user when the security of the user signature certificate has been potentially compromised (i.e.

[the revocation] may occur, for example, where an individual believes that his or her private key has been compromised) (col. 8, lines 79).

**In regards to claim 7**, Cordery teaches using the user signature certificate to authenticate the user before the creating (col. 1, lines 20-23).

Claims 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cordery in view of Grimmer as applied to claim 3 above, further in view of Tarpenning et al. (Pub No. 2002/0007454 and Tarpenning hereinafter).

**In regards to claim 5**, the combination of Cordery and Grimmer teaches the system of claim 3 as discussed above.

The combination of Cordery and Grimmer does not teach sending the user one of a password and a personal identification number (PIN) by the registration web server after the setting of the user entry.

Tarpenning teaches a system for managing security keys using a certificate (see Abstract).

Tarpenning teaches sending the user one of a password and a personal identification number (PIN) (i.e. confirmation) by the registration web server after the setting of the user entry (i.e. revocation) (figure 5, step 1025).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Cordery and Grimmer with the teachings of Tarpenning to include sending the user one of a password and a personal identification number (PIN) by the registration web server after the setting of the user entry with the motivation to guarantee that the revocation occurred (Tarpenning, par. [0043]).

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cordery in view of Grimmer in view of Tarpenning as applied to claim 5 above, in further view of Hsu et al. (U.S. Patent 5,982,898 and Hsu hereinafter).

**In regards to claim 6**, the combination of Cordery, Grimmer and Tarpenning teaches the system of claim 5 as discussed above.

The combination of Cordery, Grimmer and Tarpenning does not teach requesting a new signature certificate by the user using the directory password and one of the password and the PIN.

Hsu teaches an invention relating to certification used in connection with secure and authorized communications (cot. 1, lines 4-5).

Hsu teaches requesting a new signature certificate by the user using the directory password and one of the password and the PIN (see Figure 2).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Cordery, Grimmer and Tarpenning with the teachings of Hsu to include requesting a new signature certificate by the user using the directory password and one of the password and the PIN with the motivation to identify the requestor of the certificate (Hsu, col. 4, lines 56-64).

Claims 8 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cordery in view of Asay et al. (Pub. No. 2041/0011255 and Asay hereinafter).

**In regards to claims 8 and 27**, Cordery teaches the system of claim 1 as discussed above.



Cordery does not teach notifying a personal registration authority by a user that the user has lost the user signature certificate, the notifying occurring before the creating.

Asay discloses an invention that relates to electronic transactions, and, more particularly, to services supporting reliance on digital signature certificates and managing the risk of such certificates in an electronic transaction system [par. 0001].

Asay teaches notifying a personal registration authority by a user that the user has lost the user signature certificate, the notifying occurring before the creating (i.e. A subscriber can revoke a certificate to prevent reliance on forged digital signatures created using a compromised, e.g., lost or stolen, private key) (par. [0014])

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the system of Cordery with the teachings of Asay to include notifying a personal registration authority by a user that the user has lost the user signature certificate, the notifying occurring before the creating with the motivation to minimize the consequences of errors by the certification authority or subscriber (Asay, par [0014]).

Claims 9-11 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cordery in view of Asay as applied to claim 8 above, in further view of An et al. (U.S. Patent 6,715,073).

**In regards to claim 9**, the combination of Cordery and Asay teaches the system of claim 8 as discussed above.

The combination of Cordery and Asay does not teach that the creating and requesting are initiated by the personal registration authority.

An et al. discloses a registration system in which information about personal vaults is stored in an X.500 directory (col. 3, lines 45-46)

An et al. teaches that the creating and requesting are initiated by the personal registration authority (i.e. A registration authority running as a software application in the controller processes requests to issue, renew and revoke digital certificates issued by a certification authority using two pairs of public-private keys) (see Abstract).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Cordery and Asay with the teachings of An et al. to include that the creating and requesting are initiated by the personal registration authority with the motivation to handle the exploding growth in electronic business (col. 3, line 17).

**In regards to claim 10**, Cordery teaches requesting a personal registration authority's signature certificate to authenticate the personal registration authority before the creating (col. 1; lines 20-23).

**In regards to claims 11 and 28**, An et al. teaches that the personal registration authority is a supervisor of the user (figure 4, #32 and con. 5, lines 7-13).

Claims 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cordery in view of Asay in view of An et al. as applied to claim 10 above, in further view of Atkinson et al. (U.S. Patent 6,367,012 and Atkinson hereinafter).

**In regards to claims 12 and 13**, the combination of Cordery, Asay and An et al. teaches the system of claim 10 as discussed above.

The combination of Cordery, Asay and An et al. does not teach querying the directory after the requesting the registration web server revoke the user signature certificate to determine

Art Unit: 2131

if the personal registration authority is permitted to revoke the user signature certificate, and revoking the user signature certificate by the registration web server only if the personal registration authority is permitted to revoke the user signature certificate.

Atkinson discloses embedding certifications in executable files for network transmissions.

Atkinson teaches querying the directory after the requesting the registration web server revoke the user signature certificate to determine if the personal registration authority is permitted to revoke the user signature certificate, and revoking the user signature certificate by the registration web server only if the personal registration authority is permitted to revoke the user signature certificate (i.e. The function of Table 11 is to confirm whether an instruction to revoke or unvoke a license is authorized. The database looks up the agency's credentials in the Accountinfo column, obtaining from that the corresponding license that indicates which licenses or digital certificates this agency is allowed to revoke or unvoke. Each meta-agency has the right to grant revocation rights to child agencies that it directly licenses. As a result, the right to populate this second table is controlled by other entries in the same table.) (cot. 25, line 64 through cot. 26, line 6).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Cordery, Asay and An et al. with the teachings of Atkinson to include querying the directory after the requesting the registration web server revoke the user signature certificate to determine if the personal registration authority is permitted to revoke the user signature certificate, and revoking the user signature certificate by

the registration web server only if the personal registration authority is permitted to revoke the user signature certificate with the motivation to guarantee the integrity of the revocation process.

Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cordery in view of Asay in view of An et al. in view of Atkinson as applied to claim 13 above, in further view of Grimmer.

**In regards to claim 14**, the combination of Cordery, Asay, An et al. and Atkinson teaches the system of claim 14 as discussed above.

The combination of Cordery, Asay, An et al. and Atkinson does not teach generating a directory password for the user during creation of the user signature certificate.

Grimmer teaches generating a directory password for the user during creation of the user signature certificate (i.e. if a UserPassword attribute type was defined to hold user password information in the X.500 directory, user2 can query the directory to verify that the password it received from user1 matched the one held in the X.500 directory) (col. 4, lines 48-52).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Cordery, Asay, An et al. and Atkinson with the teachings of Grimmer to include generating a directory password for the user during creation of the user signature certificate with the motivation to provide a basis for authentication and security services (Grimmer, col. 4, lines 32-34).

Claims 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cordery in view of Asay in view of An et al. in view of Atkinson in view of Grimmer as applied to claim 14 above, in further view of Tarpenning et al. (Pub No. 2002/0007454 and Tarpenning hereinafter).

**In regards to claim 15**, the combination of Cordery, Asay, An et al., Atkinson and Grimmer teaches the system of claim 14 as discussed above.

The combination of Cordery, Asay, An et al., Atkinson and Grimmer does not teach sending the user one of a password and a personal identification number (PIN) by the registration web server after the setting of the user entry.

Tarpenning teaches a system for managing security keys using a certificate (see Abstract).

Tarpenning teaches sending the user one of a password and a personal identification number (PIN) (i.e. confirmation) by the registration web server after the setting of the user entry (i.e. revocation) (figure 5, step 1025).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Cordery, Asay, An et al., Atkinson and Grimmer with the teachings of Tarpenning to include sending the user one of a password and a personal identification number (PIN) by the registration web server after the setting of the user entry with the motivation to guarantee that the revocation occurred (Tarpenning, par. [0043]).

Claims 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cordery in view of Asay in view of An et al. in view of Atkinson in view of Grimmer in view of Tarpenning as applied to claim 15 above, in further view of Hsu.

**In regards to claim 16**, the combination of Cordery, Asay, An et al., Atkinson, Grimmer and Tarpenning teaches the system of claim 15 as discussed above.

Art Unit: 2131

The combination of Cordery, Asay, An et al., Atkinson, Grimmer and Tarpenning does not teach requesting a new signature certificate by the user using the directory, password and one of the password and the PIN.

Hsu teaches requesting a new signature certificate by the user using the directory password and one of the password and the PIN (see Figure 2).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the combination of Cordery, Asay, An et al., Atkinson, Grimmer and Tarpenning with the teachings of Hsu to include requesting a new signature certificate by the user using the directory, password and one of the password and the PIN with the motivation to identify the requestor of the certificate (Hsu, col. 4, lines 56-64).

Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cordery in view of An et al.

**In regards to claim 17**, Cordery teaches the system of claim 1 as discussed above. Cordery does not teach wherein the revoking is performed by the registration web server. An et al. teaches that the creating and requesting are initiated by the personal registration authority (i.e. A registration authority running as a software application in the controller processes requests to issue, renew and revoke digital certificates issued by a certification authority using two pairs of public-private keys) (see Abstract).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the system of Cordery with the teachings of An et al. to include that the revoking is performed by the registration web server with the motivation to handle the exploding growth in electronic business (cot. 3, line 17).

Claims 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cordery in view of Atkinson.

**In regards to claims 19-20,** Cordery teaches claim 18 as discussed above.

Cordery does not teach verifying the entity is permitted to revoke the user signature certificate, and revoking the user signature certificate only if the entity is permitted to revoke the user signature certificate.

Atkinson discloses embedding certifications in executable files for network transmissions.

Atkinson teaches querying the directory after the requesting the registration web server revoke the user signature certificate to determine if the personal registration authority is permitted to revoke the user signature certificate, and revoking the user signature certificate by the registration web server only if the personal registration authority is permitted to revoke the user signature certificate (i.e. The function of Table 11 is to confirm whether an instruction to revoke or unrevoke a license is authorized. The database looks up the agency's credentials in the AccountInfo column, obtaining from that the corresponding license that indicates which licenses or digital certificates this agency is allowed to revoke or unrevoke. Each meta-agency has the right to grant revocation rights to child agencies that it directly licenses. As a result, the right to populate this second table is controlled by other entries in the same table.) (col. 25, line 64 through col. 26, line 6).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the system of Cordery with the teachings of Atkinson to include verifying the entity is permitted to revoke the user signature certificate, and revoking the user .

signature certificate only if the entity is permitted to revoke the user signature certificate with the motivation to guarantee the integrity of the revocation process.

Claim 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cordery in view of An et al.

**In regards to claim 22**, Cordery teaches the server according to claim 18 as discussed above.

Cordery does not teach that the entity is a personal revocation authority.

An et al. teaches that the creating and requesting are initiated by the personal registration authority (i.e. A registration authority running as a software application in the controller processes requests to issue, renew and revoke digital certificates issued by a certification authority using two pairs of public-private keys) (see Abstract).

Therefore it would have been obvious to one of ordinary skill in the art at the time of Applicant's invention to modify the system of Cordery to include that the entity is a personal revocation authority with the motivation to handle the exploding growth in electronic business (col. 3, line 17).

**Action is Final**

**THIS ACTION IS FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period



Art Unit: 2131

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

### Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Taghi T. Arani, Ph.D.  
Examiner  
Art Unit 2131

